ISSUE 16
APRIL 2024
LOUISVILLE, TN

MONTHLY TECH TALK FROM YOUR FRIENDS AT PCS!

"Insider Tips to Make Your Business Run Faster, Easier and More Profitable"

INSIDE THIS ISSUE:

Give PCS a call today **(865-273-1960)** for a quick, non-salesy chat to find out whether my team and I can help you better secure your data and get more out of your existing technology!

- Carl Salyards
Business Development Rep.
csalyards@pcsknox.com

BE CAREFUL WHEN SCANNING QR CODES

QR codes are everywhere these days, both offline and online. They are convenient and easy to use: you scan them with your smartphone camera, and then you're directed to a link, a coupon, a video, or some other online content.

With the rise in popularity of QR codes comes an unfortunate dark side. Cybercriminals exploit this technology for nefarious purposes by creating fake QR codes to steal personal information. They can infect your device with malware or trick you into paying money. It's crucial to exercise caution when scanning QR codes as new phishing scams continue to emerge and exploit trust in QR codes.

How These Scams Work

The scammer prints out a fake QR code and places it over a legitimate one. For example, they might stick it on a poster advertising a product discount or a movie.

You scan the fake QR code, thinking it's legitimate. The phony code may direct you to a phishing website that asks you to enter sensitive data such as your credit card details, login credentials, or other personal information. It is also common when engaged with a QR code scam that the code prompts you to accidentally download a malicious app. These malware-ridden apps can do one or more of the following:

- Spy on your activity.
- Access your copy/paste history.
- Access your contacts.
- Lock your device until you pay a ransom.

The code could also direct you to a payment page that charges you a fee for something supposedly free. Below are some tactics to watch out for.

Malicious Codes Concealed

Cybercriminals tamper with legitimate QR codes, often adding fake stickers over real ones to embed malicious content or redirect users to fraudulent websites.

Fake Promotions & Contests

Scammers often use QR codes to lure users into fake promotions or contests. When users scan the code, it may direct them to a counterfeit website.

Malware Distribution

Some malicious QR codes start downloads of malware onto the user's device.

STAY VIGILANT: TIPS FOR SAFE QR CODE SCANNING

1. Verify the Source - Verify the legitimacy of the code and its source.

2. Use a QR Code Scanner App – Use a dedicated QR code scanner app rather than the default camera app on your device.

3. Inspect the URL Before Clicking – Before visiting a website prompted by a QR code, review the URL.

4. Avoid Scanning Suspicious Codes-Trust your instincts. If a QR code looks suspicious, refrain from scanning it.

5. Update Your Device and Apps Regularly- Keep your device's operating system and QR code scanning apps up to date.

6. Regularly Audit Connected Devices – Don't enter personal information on a website you accessed through a QR code, including your address, credit card details, login information, etc. Don't pay any money or make any donations through a QR code.

Unleash the power of your screens with Google Chromecast! This nifty device is not just about streaming your favorite shows; it's a productivity powerhouse!

One of its many functions is screen mirroring, which lets you share the content playing on your mobile device to a larger display. This is ideal for enhancing office collaboration, training, and presentations.

WHAT IS MICROSOFT SECURITY COPILOT?

It can be challenging to keep up with the ever-evolving cyber threat landscape. Companies need to process large amounts of data and respond to incidents quickly & effectively.

That's where Microsoft Security Copilot comes in. It is a generative AI-powered security solution that provides tailored insights that empower your team to defend your network. It also works with other Microsoft security products.

Microsoft Security Copilot helps security teams:

- Respond to cyber threats.
- Process signals.
- Assess risk exposure at machine speed.

A significant benefit is that it integrates with natural language, which means you can ask questions plainly to generate tailored guidance and insights. For example, you can ask:

- What are the best practices for securing Azure workloads?
- What is the impact of CVE-2024-23905 on my organization?
- Generate a report on the latest attack campaign.

Security Copilot can help with end-to-end scenarios such as:

- Incident response.
- Threat hunting.
- Executive summaries on security investigations.
- **How Does Microsoft Security Copilot Work?**

You can access Microsoft Security Copilot capabilities through a standalone experience and embedded experiences in other Microsoft security products.

Copilot integrates with several tools, including:

- Microsoft Sentinel.
- Microsoft Defender XDR.
- Microsoft Intune.
- Microsoft Purview.
- Microsoft Defender for Cloud.

You can use natural language prompts with Security Copilot.

Should You Use Microsoft Security Copilot?

The Pros:

1. Advanced Threat Detection.
2. Operational Efficiency.
3. Integration with Microsoft Products.
4. Continuous Learning.

The Considerations:

1. Integration Challenges.
2. Resource Requirements.
3. Training & Familiarization.

The Bottom Line:

Microsoft Security Copilot has an advanced capacity for real-time threat detection, operational efficiency, and extensive integration capabilities. These factors make it a compelling choice, especially for businesses seeking to fortify their digital defenses.

Your unique business needs should guide the decision to adopt Microsoft Security Copilot. Consider factors such as existing cybersecurity infrastructure and resource availability and the commitment to ongoing training.

CYBERSECURITY PREDICTIONS YOU SHOULD PLAN FOR IN 2024

Cybersecurity is a constantly evolving field. There are new threats, technologies, and opportunities emerging every year. Organizations must be aware of current and future cyber threats as we stand a quarter through 2024. Businesses of all sizes and sectors should plan accordingly, as staying ahead of the curve is paramount to safeguarding digital assets.

Below are some cybersecurity predictions for 2024 that you should consider:

- AI will be a Double-Edged Sword.
- Quantum Computing will become a Looming Threat.
- “Hacktivism” will rise in Prominence.
- Ransomware will Remain a Persistent Threat.
- Cyber Insurance will become more Influential.

SIGNS THAT YOUR SMART HOME DEVICE HAS BEEN HACKED

Smart home devices are becoming more popular and convenient; however, they pose some serious security risks. Hackers can target these devices to access your personal information, spy on your activities, or cause damage to your home. How can you tell if a hacker has compromised your smart home device? Here are some signs to look out for:

- Unusual Network Traffic.
- Strange Sounds or Voices.
- Device Settings Modification.
- Unexplained Data Transfers.
- Device Inaccessibility.
- New or Unknown Devices on the Network.
- Frequent Software Glitches.
- Emails or Messages Confirming Changes You Didn’t Make.

FOLLOW PCS ON SOCIAL MEDIA!

Join us on social media for your daily dose of tech inspiration! We've got everything from the latest trends to exclusive contests and giveaways. So take advantage of the fun and stay connected with the tech community!

PCS, Inc.

@PCSKnoxville

@PCSKnox

PCS, Inc.

@PCSKnox

TECHNOLOGY TRIVIA TIME!

Each month you have a chance to win a $25 Amazon Gift Card by being the first person to email us with the answer to our Tech Trivia Question of the Month! See there are perks for actually reading this thing :) The question this month is:

World-wide, what language is used the most on the Internet?

The first person to email me at bschreiber@pcsknox.com with the correct answer gets a $25 Amazon Gift Card!